This listing of claims replaces all prior versions, and listings of claims in the instant application:

Listing of Claims:

1. (Currently Amended) A method for securing a communication between a peer node and ~~an intermediary peer~~ a super peer node in a peer-to-peer network, the method comprising:

the peer node generating a secured communication request to the ~~intermediary peer node,~~ super peer node, the super peer node being a peer node that serves as an intermediary contact point for administrative information that concerns the super peer node as well as a subset of the peer-to-peer network associated with the super peer node and for which the super peer node is responsible;

the ~~intermediary peer node,~~ super peer node authenticating the peer node in response to said secured communication request, and

the ~~intermediary peer node,~~ super peer node issuing a signed certificate of authority upon successful authentication.

2. (Original) The method of claim 1 wherein said secured communication request comprises a certificate signing request, a unique identifier, and a password.

3. (Original) The method of claim 2 wherein said certificate signing request includes a public key cryptography system (PKCS) certificate signing request.

4. (Original) The method of claim 1 wherein said secured communication protocol comprises
a transport layer data authentication protocol.

5. (Currently Amended) The method of claim 1 wherein said ~~intermediary peer node,~~ super peer node is communicatively coupled to an enterprise database, said enterprise database authenticates the peer node in response to said secured communication request.

6. (Currently Amended) The method of claim 1 further comprising securing a pipe connection between the peer node and the ~~intermediary peer node,~~ super peer node upon authentication.

7. (Original) The method of claim 6 further comprising closing said pipe connection upon failed authentication of said node.

8. (Original) The method of claim 1 wherein said peer node comprises a peer node advertisement and a pipe node advertisement.

9. (Original) The method of claim 8 wherein said peer node advertisement comprises a peer node name, a unique peer node identifier, and local transport information.

10. (Original) The method of claim 8 wherein said pipe node advertisement includes an application-dependent port identifier, said unique identifier, a name, and a type.

11. (Original) The method of claim 1 wherein the peer-to-peer network operates using a JXTA technology-enabled platform.

12. (Currently Amended) A method for securing a communication between a peer node and ~~an intermediary peer node~~ a super peer node in a peer-to-peer network, the method comprising:

generating a secured communication request to the ~~intermediary peer node~~ super peer node, the super peer node being a peer node that serves as an intermediary contact point for administrative information that concerns the super peer node as well as a subset of the peer-to-peer network associated with the super peer node and for which the super peer node is responsible, the secured communication request being capable of authenticating the peer node in response to said secured communication request, and

receiving a signed certificate of authority upon successful authentication.

13. (Original) The method of claim 12 wherein said secured communication request comprises a certificate signing request, a unique identifier, and a password.

14. (Original) The method of claim 13 wherein said certificate signing request includes a public key cryptography system (PKCS) certificate signing request.

15. (Original) The method of claim 12 wherein said secured communication protocol comprises
a transport layer data authentication protocol.

16. (Currently Amended) The method of claim 12 wherein said ~~intermediate peer~~ super peer node is communicatively coupled to an enterprise database, said enterprise database authenticates the peer node in response to said secured communication request.

17. (Currently Amended) The method of claim 12 further comprising securing a pipe connection between the peer node and the ~~intermediate peer~~ super peer node upon authentication.

18. (Original) The method of claim 17 further comprising closing said pipe connection upon failed authentication of said node.

19. (Original) The method of claim 12 wherein said peer node comprises a peer node advertisement and a pipe node advertisement.

20. (Original) The method of claim 19 wherein said peer node advertisement comprises a peer node name, a unique peer node identifier, and local transport information.

21. (Original) The method of claim 19 wherein said pipe node advertisement includes an application-dependent port identifier, said unique identifier, a name, and a type.

22. (Original) The method of claim 12 wherein the peer-to-peer network operates using a JXTA technology-enabled platform.

23. (Cancelled) Please cancel Claim 23, without prejudice.
A method for securing a communication between a peer node and an intermediary peer node in a peer-to-peer network, the method comprising:

receiving a secured communication request from the peer node;

authenticating the peer node in response to said secured communication request; and

sending a singed certificate of authority upon successful authentication.

24. (Cancelled) Please cancel Claim 24, without prejudice. The method of claim 23 wherein said secured communication request comprises a certificate signing request, a unique identifier, and a password.

25. (Cancelled) Please cancel Claim 25, without prejudice. The method of claim 24 wherein said certificate signing request includes a public key cryptography system (PKCS) certificate signing request.

26. (Cancelled) Please cancel Claim 26, without prejudice. The method of claim 23 wherein said secured communication protocol comprises
a transport layer data authentication protocol.

27. (Cancelled) Please cancel Claim 27, without prejudice. The method of claim 23 wherein said intermediate peer node is communicatively coupled to an enterprise database, said enterprise database authenticates the peer node in response to said secured communication request.

28. (Cancelled) Please cancel Claim 28, without prejudice. The method of claim 23 further comprising securing a pipe connection between the peer node and the intermediary peer node upon authentication.

29. (Cancelled) Please cancel Claim 29, without prejudice. The method of claim 28 further comprising closing said pipe connection upon failed authentication of said node.

30. (Cancelled) Please cancel Claim 30, without prejudice. The method of claim 23 wherein said peer node comprises a peer node advertisement and a pipe node advertisement.

31. (Cancelled) Please cancel Claim 31, without prejudice. The method of claim 30 wherein said peer node advertisement comprises a peer node name, a unique peer node identifier, and local transport information.

32. (Cancelled) Please cancel Claim 32, without prejudice. The method of claim 30 wherein said pipe node advertisement includes an application-dependent port identifier, said unique identifier, a name, and a type.

33. (Cancelled) Please cancel Claim 33, without prejudice. The method of claim 23 wherein the peer-to-peer network operates using a JXTA technology-enabled platform.

34. (Currently Amended) A program storage device readable by a machine, tangibly embodying a program of instructions executable by the machine to perform a method for securing a communication between a peer node and ~~an intermediary peer~~ a super peer node in a peer-to-peer network, the method including:

the peer node generating a secured communication request to the ~~intermediary peer~~ super peer node, the super peer node being a peer node that serves as an intermediary contact point for administrative information that concerns the super peer node as well as a subset of the peer-to-peer network associated with the super peer node and for which the super peer node is responsible;

the ~~intermediary peer~~ super peer node authenticating the peer node in response to said secured communication request, and

the ~~intermediary peer~~ super peer node issuing a signed certificate of authority upon successful authentication.

35. (Currently Amended) A program storage device readable by a machine, tangibly embodying a program of instructions executable by the machine to perform a method for administrating peer-to-peer networks, the method including:

generating a secured communication request to ~~an intermediary peer~~ a super peer node, the super peer node being a peer node that serves as an intermediary contact point for administrative information that concerns the super peer node as well as a subset of the peer-to-peer network associated with the super peer node and for which the super peer node is responsible, the secured communication request being capable of authenticating the peer node in response to said secured communication request, and

receiving a signed certificate of authority upon successful authentication.

36. (Currently Amended) A program storage device readable by a machine, tangibly embodying a program of instructions executable by the machine to perform a method for administrating peer-to-peer networks, the method including:

~~an intermediary peer~~ a super peer node receiving a secured communication request from a peer node, the super peer node being a peer node that serves as an intermediary contact point for administrative information that concerns the super peer node as well as a subset of the peer-to-peer network associated with the super peer node and for which the super peer node is responsible;

authenticating the peer node in response to said secured communication request; and

sending a signed certificate of authority upon successful authentication.

37. (Currently Amended) An apparatus for securing a communication between a peer node and ~~an intermediary peer~~ a super peer node in a peer-to-peer network comprising:

means for generating a secured communication request to the ~~intermediary peer~~ super peer node, the super peer node being a peer node that serves as an intermediary contact point for administrative information that concerns the super peer node as well as a subset of the peer-to-peer network associated with the super peer node and for which the super peer node is responsible;

means for authenticating the peer node in response to said secured communication request, and

means for issuing a signed certificate of authority upon successful authentication.

38. (Currently Amended) An apparatus for securing a communication between a peer node and ~~an intermediary peer~~ a super peer node in a peer-to-peer network comprising:

means for generating a secured communication request to the ~~intermediary peer~~ super peer node, the super peer node being a peer node that serves as an intermediary contact point for administrative information that concerns the super peer node as well as a subset of the peer-to-peer network associated with the super peer node and for which the super peer node is responsible, the secured communication request being capable of authenticating the peer node in response to said secured communication request, and means for receiving a signed certificate of authority upon successful authentication.

39. (Cancelled) Please cancel Claim 39, without prejudice. An apparatus for securing a communication between a peer node and an intermediary peer node in a peer-to-peer network comprising:

means for receiving a secured communication request from the peer node;

means for authenticating the peer node in response to said secured communication request; and

means for sending a signed certificate of authority upon successful authentication.

40. (Currently Amended) A peer-to-peer network system comprising:

a peer node;

~~an intermediary peer~~ a super peer node communicatively coupled to said peer node, the super peer node being a peer node that serves as an intermediary contact point for administrative information that concerns the super peer node as well as a subset of the peer-to-peer network associated with the super peer node and for which the super peer node is responsible;

wherein said peer node is configured to generate a secured communication request to said ~~intermediary peer~~ super peer node;

wherein said ~~intermediary peer~~ super peer node is configured to authenticate said peer node in response to said secured communication request, and

wherein said ~~intermediary peer~~ super peer node is configured to issue a signed certificate of authority upon successful authentication.

41. (Currently Amended) A peer node comprising:

a processor; and

a memory comprising program instructions, wherein the program instructions are executable by the processor to:

generate a secured communication request to ~~an intermediary peer~~ a super peer node, the super peer node being a peer node that serves as an intermediary contact point for administrative information that concerns the super peer node as well as a subset of the peer-to-peer network associated with the super peer node and for which the super peer node is responsible, the secured communication request being capable of authenticating the peer node in response to said secured communication request, and

receive a signed certificate of authority upon successful authentication.

42. (Cancelled) Please cancel Claim 42, without prejudice. An intermediary peer node comprising:

a processor; and

a memory comprising program instructions, wherein the program instructions are executable by the processor to:

receive a secured communication request from an peer node;

authenticate the peer node in response to said secured communication request; and

send a signed certificate of authority upon successful authentication.